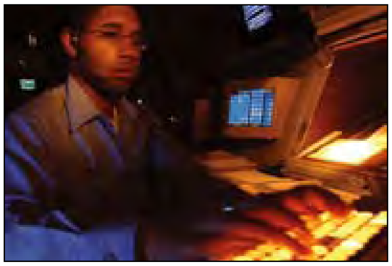
CWID 2007 DEMONSTRATION

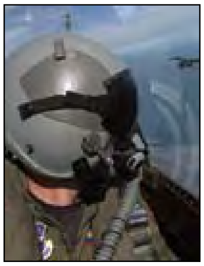
Guidebook Contents

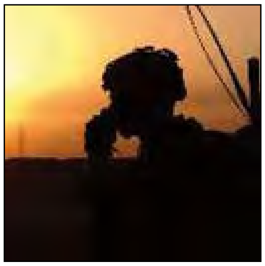
Published May 2007
Defense Information Systems Agency (DISA) CWID Joint Management Office (JMO)
Arlington, Va., and Hampton, Va.
For information or to obtain copies, contact: CWIDPA@langley.af.mil

www.cwid.js.mil

NOTES



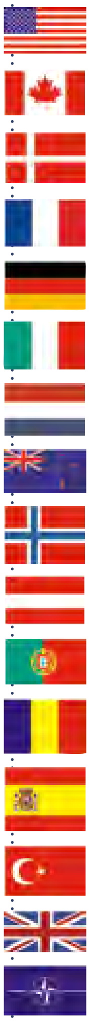




CWID 2007 DEMONSTRATION

Executive Summary

CWID is the Chairman of the Joint Chiefs of Staff's annual event enabling combatant commanders and the international community to investigate command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) solutions that focus on relevant and timely objectives for enhancing coalition interoperability. CWID investigates information technologies that will integrate into an operational environment within the near term following demonstration execution every year in June.



All those involved, commercial and government sectors, take some risk to realize substantial benefits. Potential technology developers bring hardware, software and package solutions to the CWID venue for evaluation. Combatant commands, services, DoD and other government agencies investigate new and emerging technologies and parallel tactics, techniques, and procedures (TTP), employing the scenario and controlled operational environment for low-threat analysis.

While the focus of CWID is on new and emerging technologies, CWID is also a venue for information technology development or validation of fielded or near-fielded commercial, DoD and partner systems (those already in the research and development [R&D] and acquisition pipeline) to reduce fielding costs or programmed transition timelines.

Defense Information Systems Agency (DISA) engineers a global network during the demonstration with participating trial assessment nodes at: Naval Surface Warfare Center, Dahlgren Division (NSWCDD), Dahlgren, Va. (U.S. Army and Marine Corps site); Space and Naval Warfare Systems Command (SPAWAR), San Diego, Calif. (U.S. Navy site); Electronic Systems Center, Hanscom Air Force Base, Mass. (U.S. Air Force site); and two combatant commander sites, U.S. European Command (USEUCOM), Stuttgart, Germany; and U.S. Northern Command (USNORTHCOM), Colorado Springs, Colo. Coalition partners bring more than 25 additional sites to the temporary isolated network.

OBJECTIVES

1. CROSS-DOMAIN DATA SHARING

2. INTEGRATED INTELLIGENCE

3. INTEGRATED OPERATIONS

4. INTEGRATED LOGISTICS

5. INTEGRATED PLANNING

6. INTEGRATED COMMUNICATIONS

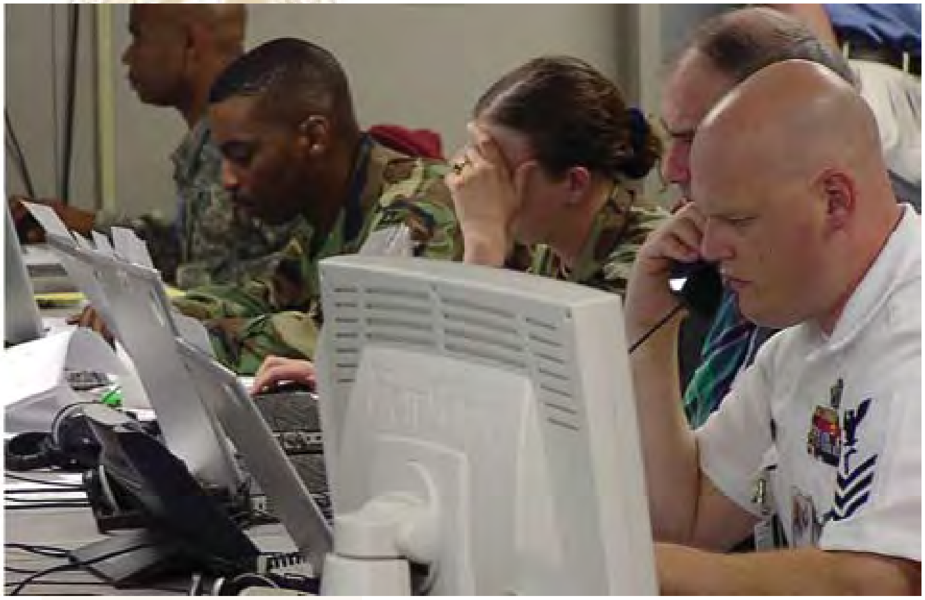
(Expanded objrctive information and detail follows on page 5)

One more U.S. site on the network, newly established for the 2007 demonstration, is located in the Pentagon. The Warfighter Capability Demonstration Center (WarCap), will provide an interactive window to U.S. trial sites for senior decision makers inside the Pentagon and in the Capitol region.

CWID management is committed to the concept that all multinational information sharing solutions should be built on a foundation that is net-centric, secure, scalable, and bandwidth sensitive.

Coalition participation remains the cornerstone of CWID. Interoperability trials with coalition partners are hosted over a worldwide secure network, enabling classified, releasable data to be exchanged among Canada, New Zealand, United Kingdom, NATO, and Partnership for Peace nations. U.S. combatant commanders may invite other nations, from their respective areas of responsibility, to participate as multinational task force (MTF) members. For example, U.S. Pacific Command (USPACOM) involved Pacific Rim nations through 2005.

Depending on demonstrated capabilities and based on planning-documentation criteria, each information technology trial may receive one or more assessments: Warfighter/Operator; Technical/Interoperability; and Security



Capabilities. The Systems Engineering and Integration Working Group (SEIWG), with input from other working groups, reports on interoperability trials not formally assessed by the Assessment Working Group (AWG). Results from assessments are documented in a final report published by October every year.

U.S. Joint Forces Command (USJFCOM), on behalf of the Chairman, is responsible for oversight of CWID, a natural fit for the command's mandate to equip U.S. military forces. The USJFCOM Capability Development Process is the primary method used to identify candidate technologies through the CWID initial selection process and after demonstration results are formalized.

USEUCOM is host combatant commander for CWID 2006-2008. Headquartered in Stuttgart, Germany, the command brings an *in situ* coalition emphasis. The scenario describes notional coalition task force operations applicable in the Global War on Terrorism (GWOT) with terrorist backlash and natural disasters for USNORTHCOM's Homeland Security and Homeland Defense (HS/HD) component.

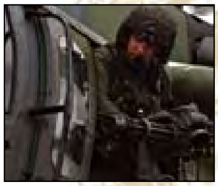
CWID supports USNORTHCOM transformational efforts, providing investigation of systems integration and interoperability solutions in the first-responder arena. This includes USNORTHCOM's interagency partners, the Department of Homeland Security(DHS) and Public Safety Emergency Preparedness Canada. National Guard Bureau state units are participating in 2007 with two live exercise sites, Mountaineer CWID, W.Va., and Palmetto CWID, Charleston, S.C. Delaware, Colorado, California, Massachusetts, and New York units are supporting DoD sites with role players and operators for HS/HD scenario events.

Yearly process improvements facilitate development of strategies aimed at responsibly bringing technology solutions to the DoD Acquisition, Technology and Logistics (AT&L) community for consideration.

The CWID Senior Management Group (SMG), together with coalition partners, selects interoperability trial proposals to satisfy information sharing required among military organizations, international coalitions and civilian agencies. Selection criteria is based on how well a potential trial's proposal satisfies one or more published objectives defined by the host combatant commander.

CWID demonstrations support the overall Network Centric Warfare (NCW) construct, leveraging advantages of emerging technology. During the demonstration execution phase, trials are conducted over, or connected to, a global network that supports military and coalition operations while providing infrastructure for Defense Support to Civil Authorities (DSCA). The CWID Joint Management Office (JMO), under DISA direction, coordinates, engineers, and supervises the network backbone(s), information domains and the worldwide venue, providing interoperability trial assessments in the Final Report.

Yearly process improvements facilitate development of strategies aimed at responsibly bringing technology solutions to the DoD Acquisition, Technology and Logistics (AT&L) community for consideration. CWID management is committed to the concept that all multinational (DoD and non-DoD entities) information sharing solutions should be built on a foundation that is net-centric, secure, scalable, and bandwidth sensitive.



CWID 2007 OBJECTIVES

Objectives Identify Gaps

CWID 2007 charged that information sharing solutions should be built on a foundation that is net-centric, secure, scalable, and bandwidth sensitive.

CWID 2007 objectives described below contain key differences from those associated with past Joint/Coalition Warrior Interoperability Demonstrations.

Objectives are focused to reflect the following recurring themes: investigating emerging and relevant technologies; focus CWID on demonstrating solutions for combatant command theater capability gaps and challenges; enhance multi-service, multinational, and inter-agency cooperation and communication.

OBJECTIVE 1. CROSS DOMAIN DATA SHARING

Provide capability to share information across multiple networks of potentially different security classifications and caveats. Emphasis is on passing information to U.S. controlled, coalition networks such as Combined Enterprise Regional Information Exchange Systems (CENTRIXS) network, and coalition/alliance controlled networks such as Northern Atlantic Treaty Organization (NATO) Initial Data Transfer System (NIDTS), NATO Mission Wide Area Network. Data sharing encompasses the need for cross-domain solutions (CDS) and the assurance that information passed through CDS can be utilized by systems within all security enclaves.

■ Improve information sharing capability through secure use of operating systems and applications to facilitate battle planning and information dissemination.

1. Provide secure means for system-to-system communications across domains.

2. Provide secure means to conduct a complete suite of collaboration activities across domains.

3. Provide secure means for one-way and two-way file sharing across domains to include protection from malicious code and data leakage.

4 Provide a secure intrusion detection solution for monitoring cross domain activities.

■ Improve CDS implementation at the tactical versus operational level, recognizing that the applications are different through echelons of command.

EXPLANATION: Coalition operations require an information environment that spans multiple Communities of Interest (COI) where C/S/As are likely affected by limited bandwidth. Within any COI, mission success relates to the commander's command and control (C2) ability to communicate directly with individual users or first responders who may be detached from fixed information domains.

Objective numbering reflects approximate linkage to traditional U.S. military staff codes.

■

Objectives are supported by sub-objectives referenceing clearly defined U.S. combatant command and coalition capability gaps.

■

Objectives are linked to the Joint Battle Management Command and Control Roadmap and Joint Mission Threads.

OBJECTIVE 2. INTEGRATED INTELLIGENCE

Provide solutions that improve the commander's ability to share intelligence information products (documents, images, databases, etc.) with coalition partners, including joint and coalition forces, government agencies, NGOs, and first responders.

■ Improve rapid situational awareness of the area of operations utilizing advanced visualization technologies..

1. Demonstrate the ability to ingest geospatial data and display sophisticated 3D imagery that identifies all the elements of national resources, including political hotspots, military presence, economic icons, social, public works infrastructure, and other pertinent information.

2. Demonstrate a robust visualization architecture that supports common open application program interfaces using approved international standards and DoD approved data formats and ports/protocols.

■ Enhance the maritime common operational picture (COP) through the intelligent retrieval and fusion of data from disparate sources, population of empty track fields, analysis and detection of anomalous track behaviors and uncovering operator errors.

■ Develop customized, adaptable, dynamic, scalable intelligence estimates.

■ Develop sensor capability that automatically stores and retrieves significant events to assist the conventional forces and first responders.

■ Demonstrate fusion analysis in which computer systems and software are used to extract and compare multiple sources of information and databases.

EXPLANATION: Coalition information sharing must be secure, scaleable in scope and functional within the theater bandwidth available at all levels of warfare. Trial proposals should be capable of using existing interface standards and protocols that define the format, content, and exchange mechanisms for shared data.

OBJECTIVE 3. INTEGRATED OPERATIONS

Enhance the commander's capability to command, control, and coordinate across joint and coalition forces, government agencies, NGOs, and first responders.

- Demonstrate new technology or enhancement to existing technology that streamlines the operational decision-making process throughout the spectrum of military and civil operations, including GWOT contingencies and crisis response.
- Improved blue force tracking identification capability across multiple enclaves.
- Situational awareness using advanced visualization technologies (see Objective 2).
- Cross and secure spectrum interface capabilities for tactical/commercial radios.
- Common collaboration tool suite that is accepted by joint/conventional forces and HLS/HLD entities.
- Improved red force tracking capability across mission areas and user communities.
- Improved non-material solutions, specifically tactics, techniques, and procedures to task, discover, fuse and use Global Information Grid (GIG)-enabled products
- Shifting the focus at the operational level to long-term integration of tactical operations with specific nation-building forces and capabilities.
- Increasing tactical autonomy and decentralization.
- Providing and sharing cultural and social awareness to a level approaching situational awareness.
- Improving mobility, survivability and adaptive dominance.
- Achieving a joint/coalition integrated fire control system of systems.
- Defending effectively against the use of Electro Magnetic Pulse (EMP) or Weapons of Mass Destruction (WMD).

EXPLANATION: Integrated Operations imply that coalition, military and civilian authorities can harness the power of their respective information environments to collaboratively execute operations even in a bandwidth-constrained environment. Information exchange between these COIs must inspire confidence at each activity that the information is being disseminated securely, and will be available to agreed upon and authorized participants.

OBJECTIVE 4. INTEGRATED LOGISTICS

Demonstrate ability to access and consolidate logistical information across organizational boundaries to assess and display, in near real time, information on the movement, location and status of joint forces, military services, interagency, coalition, NGO and first responder equipment, supplies and personnel en route, and/or deployed.

- Improve logistics data access, fusion and integration among COIs.
- Improve distributed operations, operational agility, distributed support and sustainment, and exploitation of the vertical dimension of sustainment thereby reducing logistical infrastructure in-theater.

EXPLANATION: Within the information environment, the commander must have responsive and effective logistics. Logistic data is contained within diverse logistics information systems maintained by the military and civilian agencies across the coalition. Access to that data implies combining total asset visibility and information during the transit of friendly forces into a single information presentation available across multiple information COIs.

OBJECTIVE 5. INTEGRATED PLANNING

Provide solutions that improve the combatant commander's ability to conduct collaborative planning with coalition partners, including joint and coalition forces, government agencies, NGOs and first responders.

- Improve sharing capabilities that support Essential Elements of Information (EEIs) for forces supporting CTF and HLS/HLD scenarios.
- Evaluate technologies and processes that support collection and dissemination of Command and Control (C2) information using Net Centric Enterprise Services (NCES).

EXPLANATION: Integrated Planning implies that coalition, military, and civilian authorities can harness the power of their respective information environments to collaboratively plan operations even in a bandwidth-constrained environment. Collaborative planning and dissemination of products in a bandwidth constrained environment horizontally across and vertically within COIs is an emerging issue for the warfighter, particularly as software and procedure tools become sufficiently robust to be extended from the operational to the tactical level of warfare.

OBJECTIVE 6. INTEGRATED COMMUNICATIONS

Robust, joint and combined, interoperable and multilingual information sharing capabilities improve decision making and planning among Allied and coalition partners and other bandwidth-disadvantaged users.

- Translation Services: Provide solutions that improve the combatant commander's ability to share information with and receive information from multi-lingual coalition partners,.
- Identify and evaluate an allied/coalition directory services architecture that facilitates the sharing of information among coalition nations.
- Create an interoperable interface between Service tactical radios and Coalition tactical radios.

  1. Improve interoperability between United States Marine Crop (USMC) tactical Ultra High Frequency/Very High Frequency (UHF/VHF) radios in the frequency hopping mode and the USMC High Frequency (HF) radio with a Coalition suite of radios in the secure mode.
  2. The suite of radios need to be the communication medium between the US Army Advanced Field Artillery Tactical Data System (AFATDS), the USMC AFATDS, the U.S. Navy's Naval Fire Control System, and Coalitions like system.
  3. Identify and assess Voice over Internet Protocol (VoIP) solutions suitable for use over maritime tactical networks.
  4. Identify National Security Agency's high assurance internet protocol encryption devices to support CDS and coalition information sharing.
  5. Demonstrate domain controlled data protection at rest in a multi-domain coalition environment.
  6. Demonstrate Network Defense Situational Awareness and advanced anomaly detection technologies in a multi-domain coalition environment.

EXPLANATION: Communications in a CWID context is interpreted as coalition information sharing, and is more than providing a radio communication or common operational picture at or between the strategic, operational, or tactical level of command. It must be secure, scaleable in scope and functional within the theater bandwidth available at all levels of warfare.

LEAD COMMANDER

U.S. European Command

As the only forward deployed regional combatant command with a headquarters outside the United States, U.S. European Command (USEUCOM) is currently charged with a 92-country area of responsibility spanning from the North Atlantic across Europe and Russia down to the tip of South Africa. The command maintains ready forces to conduct the full range of operations, unilaterally or in concert with coalition partners, to promote regional stability, counter terrorism, and enhance transatlantic security through support of NATO.

USEUCOM envisions Europe as a global partner, a self-sufficient and stable Africa, a broader Middle East at peace, capable regional security organizations, and a transformed and expeditionary USEUCOM and NATO. Leveraging new technologies and coalition interoperability is absolutely crucial to enabling these visions in this dynamic environment, an environment bringing big changes to the USEUCOM future. As of fall 2007, U.S. Africa Command (USAFRICOM) will assume responsibility for the continent of Africa. As the USEUCOM mission changes, the need for technological innovation and interoperability increases. USEUCOM is proud to have been the host combatant command for CWID 2006 and to continue hosting for 2007 and 2008.

CONTACTS

Maj Kevin Westley
CWID Branch Chief
CML +49-711-680-6583
DSN 314-430-6583

CDR Greg Stephens
CML +49-711-680-4364
DSN 314-430-4364

LCDR Mark Christensen
CML +49-711-680-4895
DSN 314-430-4895

cwid@eucom.mil

2008 Objectives

OBJECTIVE 1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE

This objective will enhance leadership's capability to command, control and coordinate across joint & coalition forces, government agencies, non-governmental organizations (NGOs) and first responders.

TECHNOLOGIES WILL:

- Demonstrate cohesive command and control (C2) linkages between military, government agencies and coalition partners,
- Demonstrate enhanced interoperability for NATO Response Force C2,
- Demonstrate open & secure mobile C2 capabilities between communities of interest (COIs),
- Demonstrate communication tools that streamline decision-making and integrate with existing systems or that present entirely new solutions,
- Demonstrate communication tools that share Chemical Biological Radiological Nuclear Explosive (CBRNE) contingency information with first responders & emergency services,
- Demonstrate improved general Identification and Blue Force tracking capabilities,
- Demonstrate counter insurgency Indications and Warning tools,
- Demonstrate targeting tools for non-lethal weapons and corresponding Margin of Error (MOE),
- Demonstrate systems to rapidly extend communications in support of Defense Support to Civil Agencies (DSCA) operations,
- Demonstrate tools to support neutralization of Improvised Explosive Devices (IEDs),
- Demonstrate expanded integration of open-source tools to open standards Service Oriented Architectures (SOAs), and
- Demonstrate tools to support the entire deployment process from requirements identification through force closure, including redeployment and rotational operations.

EXPLANATION: Improved C4ISR Architecture will aid coalition, military and civilian authorities to harness the power of their respective information environments to collaboratively execute operations even in a bandwidth-constrained environment.

OBJECTIVE 2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS

Provide the capability to share information across multiple networks of potentially different security classifications and caveats. Emphasis should be on passing information to both U.S.-controlled, coalition networks such as U.S. Central Command's Combined enterprise Regional Information Exchange System (CENTRIXS) and coalition/alliance controlled networks such as NATO's Initial Data Transfer System (NIDTS), NATO Mission Wide Area Network (WAN), or releasable to Republic of Korea (RELROK). Data sharing encompasses the need for cross-domain solutions (CDS) and the assurance that information passed through CDS can be utilized by systems within all security enclaves.

TECHNOLOGIES WILL:

- Demonstrate multi-level security & multi-domain applications that promote information sharing with planned and unanticipated mission partners,
- Demonstrate effective network defense applications to protect shared data,
- Demonstrate tools that improve utility, accuracy and timeliness of real time translation for collaboration in specific areas of responsibility (AORs),
- Demonstrate complementary planning tools that support military, local law enforcement, first responders, governmental, non-governmental and coalition planning activities,
- Demonstrate tools to improve Request for Forces (RFF) process,
- Demonstrate tools to improve deployment and visibility of coalition and/or interagency/Private Voluntary Organization (PVO)/NGO forces, and
- Demonstrate use of free-ware and share-ware open standards capabilities to fully connect civilian and military planners.

EXPLANATION: Coalition operations require an information environment that spans multiple COIs. These COIs may be mobile, fixed or remotely located where the combination of military and/or civil agencies is likely to be affected by limited bandwidth.

OBJECTIVE 3. ENHANCE CROSS DOMAIN AND MULTIPLE SECURITY LEVEL INFORMATION EXCHANGE TOOLS

Provide solutions that improve the commander's ability to share intelligence information products (documents, images, databases, etc.) with coalition partners, including joint and coalition forces, government agencies, NGOs and first responders.

TECHNOLOGIES WILL:

- Demonstrate data fusion tools that support cross domain information sharing and consolidates multiple sources of information into a single reference source,
- Demonstrate situational awareness tools that disseminate and display time critical information for tactical forces and first responders to include defense against IEDs,
- Demonstrate visualization and integration tools that can simultaneously manage multiple Intelligence, Surveillance and Reconnaissance inputs, and
- Demonstrate capabilities to enhance Maritime Domain Awareness between Federal, State and local agencies.

EXPLANATION: Cross domain and multiple security level information exchange represent more than providing a common operational picture at the strategic or major echelon level of command. Exchange tools must be secure, scaleable in scope and functional within the theater bandwidth available at all levels of warfare.

OBJECTIVE 4. ENHANCE INTEGRATED LOGISTICS PLANNING TOOLS

Demonstrate the ability to access, consolidate and display logistical information to include movement, location and status of joint forces, military services, interagency, coalition, NGO, first responders as well as equipment and supplies in near real time across organizational boundaries.

TECHNOLOGIES WILL:

- Demonstrate secure abilities to assess & display information regarding the movement, location, & status of Coalition equipment & personnel,
- Demonstrate logistics data access, fusion, & integration among COIs,
- Demonstrate Logistic data sharing for medical and health protection services, and
- Demonstrate capability to exchange logistic data between government agencies, NGOs and military systems.

EXPLANATION: Within the information environment of coalition, military and non-military operations, the commander must have responsive and effective logistics.

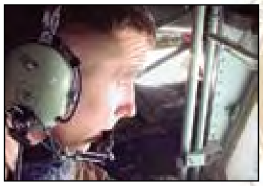
OBJECTIVE 5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY

Provide solutions that improve a Combatant Commander's ability to conduct collaborative planning with coalition partners, including joint and coalition forces, government agencies, NGOs and first responders. Focus is on enhanced collaboration and engendering a "need to share" vice a "need to know" culture.

TECHNOLOGIES WILL:

- Demonstrate data access, fusion & integration among joint forces, international, Federal and State Agencies & local law enforcement,
- Demonstrate the ability to distribute and track key policy and strategy documents between government agencies,
- Demonstrate tools to improve Information Assurance and posture between government agencies,
- Demonstrate a situational awareness tool that uses advanced visualization technologies capable of integrating existing systems into one common operational picture,
- Demonstrate a Blue Force tracking capability for first responders,
- Demonstrate computer network defense (CND) capabilities to support non-military partners,
- Demonstrate computer network capabilities that support collaboration with the Department Homeland Security Emergency Management COI, and
- Demonstrate interoperability between international agency systems and DoD, multinational systems to support Global Disaster Relief efforts.

EXPLANATION: Government agency interoperability implies that coalition, military and civilian authorities can harness the power of their respective information environments to collaboratively solve problems and plan operations even in a bandwidth-constrained environment.



NORTH AMERICAN AEROSPACE DEFENSE - U.S. NORTHERN COMMAND

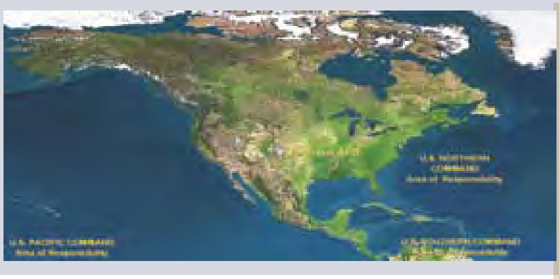
Homeland Security and Homeland Defense Commander

As a result of the events of Sept. 11, 2001, the President established a regional combatant command to en-sure military defense of the homeland and to coordinate Total Force efforts toward that end. For the first time since George Washington and the Continental Army, the United States has a military command that focuses solely on homeland defense and support to homeland security. U.S. Northern Command's (USNORTHCOM) challenge is to harness the many capabilities and skills of the Total Force to complement those of the various federal, state, tribal, and local governments and agencies, as well as the commercial and private sector, into one coherent defensive effort. USNORTHCOM will work with its key interagency partners to identify new ways to do business that improve cooperation, coordination and information sharing. New technologies will be embraced and harnessed to support the command's common purpose.

CONTACTS

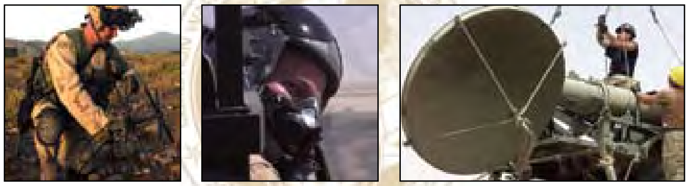
HS/HD PROGRAM MANAGER
Mr. Chris Lambert
719.554.8064
DSN 692.8064
christopher.lambert@northcom.mil

SITE MANAGER
Ms. Annette Guerrero
719.554.2802
DSN 692.2802
annette.guerrero@northcom.mil



PRIMARY MISSION

Deter attacks against the United States, its territories, possessions and bases and employ appropriate force should deterrence fail.

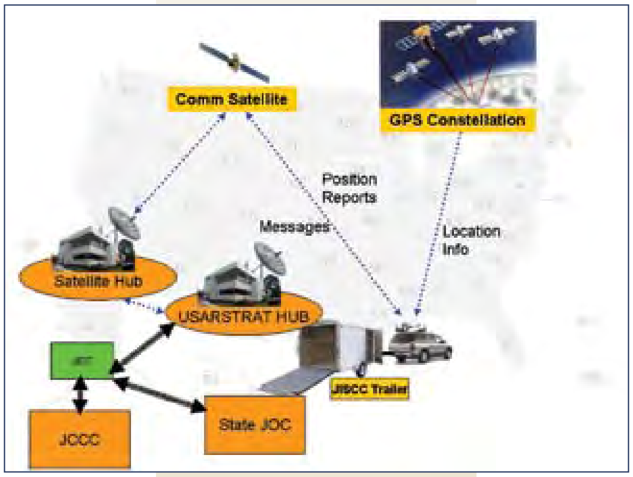


NATIONAL GUARD BUREAU

Net-Centric First Response

The National Guard's number one priority is the security and defense of our homeland, at home and abroad, and to support the Global War on Terrorism here and abroad. America insists on a relevant, reliable and ready National Guard that is transformed for the 21st Century.

The National Guard continues to expand its participation at CWID to further develop the Joint CONUS Communications Support Environment (JCCSE) with its mission partners. For CWID 2007, the National Guard will be operating notional state Joint Force Headquarters (JFHQs) and Joint Task Forces, as well a National Guard Bureau Joint Operations Center (JOC) at four CWID demonstration sites. The Delaware, Colorado, California, Massachusetts, and New York National Guard will be supporting the roleplayers and operators required to execute the National Guard scenario events. In addition, the National Guard will be supporting two state demonstration sites: Mountaineer CWID in West Virginia and Palmetto CWID in South Carolina. For more information on these state demonstration sites, see the U.S. Sites and Agencies section.



C4 ASSET TRACKING COMPONENT OF E-COP

The JCCSE is the Chief National Guard Bureau's strategic IT priority and concept driving joint C4 capability requirements and enhancements. The mission of JCCSE encompasses all of the vital organizations and net-centric IT capabilities required by the National Guard to support U.S. Northern Command (USNORTHCOM), U.S. Pacific Command (USPACOM), U.S. Strategic Command (USTRATCOM), and other Homeland Defense and Defense Support to Civil Authorities (HD/DSCA) agencies. CWID will help the National Guard test and assess newly developed JCCSE capabilities as well as explore interoperability solutions to enhance future information sharing and collaboration capabilities to and from the national level, the 54 States and Territories, and local incident sites.

Specifically, the National Guard will leverage CWID scenarios and simulated operational networks to test improved operations and coordinated HD/DSCA response. The entities involved are:

- ■ NGB Joint Operations Center
- ■ NGB Joint C4 Coordination Center (JCCC)
- ■ Joint Force Headquarter – State (JFHQ-S)
- ■ Joint Task Force – State (JTF-S)
- ■ National Guard Communications Element (NGCE) / Joint Incident Site Communications Capability (JISCC)

NATIONAL GUARD MANAGED TRIALS

The NGB is managing two interoperability trials - Next Generation Joint Information Exchange Environment (NG-JIEE) and Event-based Common Operational Picture (NG-ECOP) at CWID 2007 to support the following:

- ■ Demonstration of event-driven situation reporting capabilities that support sharing of Essential Elements of Information (EEIs) among agencies and deployed forces supporting HLD/DSCA missions
- ■ Enable the National Guard Joint C4 Coordination Center (JCCC) to improve coordination and employment of C4 Assets in response to multiple events.
- ■ Development of a National Guard COP that provides GIS-based visualization of common operational event, mission, and asset data, and supports strategic decision making

The National Guard is also assessing and supporting several other trials related to National Guard requirements for cross domain information sharing, COP Integration, interagency alerting, netcentric enterprise services, collaboration, decision support, and incident area communications.

THE NATIONAL GUARD IS SUPPORTING TWO STATE DEMONSTRATION SITES

Mountaineer CWID, West Virginia, and Palmetto CWID, South Carolina.

For more information on these sites, see the U.S. Sites and Agencies section, page 19.

CONTACT

The National Guard Bureau
1411 Jefferson Davis Highway
Arlington VA 22202-3231

Mr. Frank Monk
Assistant NGB CIO
frank.monk@ngb.ang.af.mil
301.607.5403
DSN: 327.5403

Joint Information Exchange Environment (JIEE)

MAJ Kory Gacono
C4 Integration, Program Manager
kory.gacono@ngb.ang.af.mil
703.601.2591
DSN: 329.2591

U.S. JOINT FORCES COMMAND

CWID Oversight Command

United States Joint Forces Command (USJFCOM) exercises oversight responsibility for the yearly planning and execution of the CWID.

USJFCOM assumed oversight responsibility for CWID planning and execution cycles in 2005. Concurrent with that responsibility, USJFCOM established a partnership with Allied Command-Transformation (ACT) to manage CWID and resolve national, alliance, and coalition interoperability issues as forcing agents for change.

On behalf of the Chairman of the Joint Chiefs of Staff, and in coordination with the host combatant command, USJFCOM consolidates, formulates and drafts overarching objectives derived from the nine combatant commands' integrated priority lists, USJFCOM Joint Transformation Roadmap, USJFCOM Warfighter Challenges, as well as NATO and the Combined Communications Electronics Board (CCEB) nation's interoperability issues. Incorporation of service and coalition related challenges in the overarching objectives ensures a tighter alignment of C4ISR interoperability trials and their resulting solutions.

COMMAND SECURITY OFFICE INFORMATION FOR HAMPTON ROADS

Norfolk Commander USJFCOM
1562 Mitscher Ave., Suite 200

ATTN: JOSM
Norfolk, VA 23551-2488
757.836.6405
FAX 757.836.6366

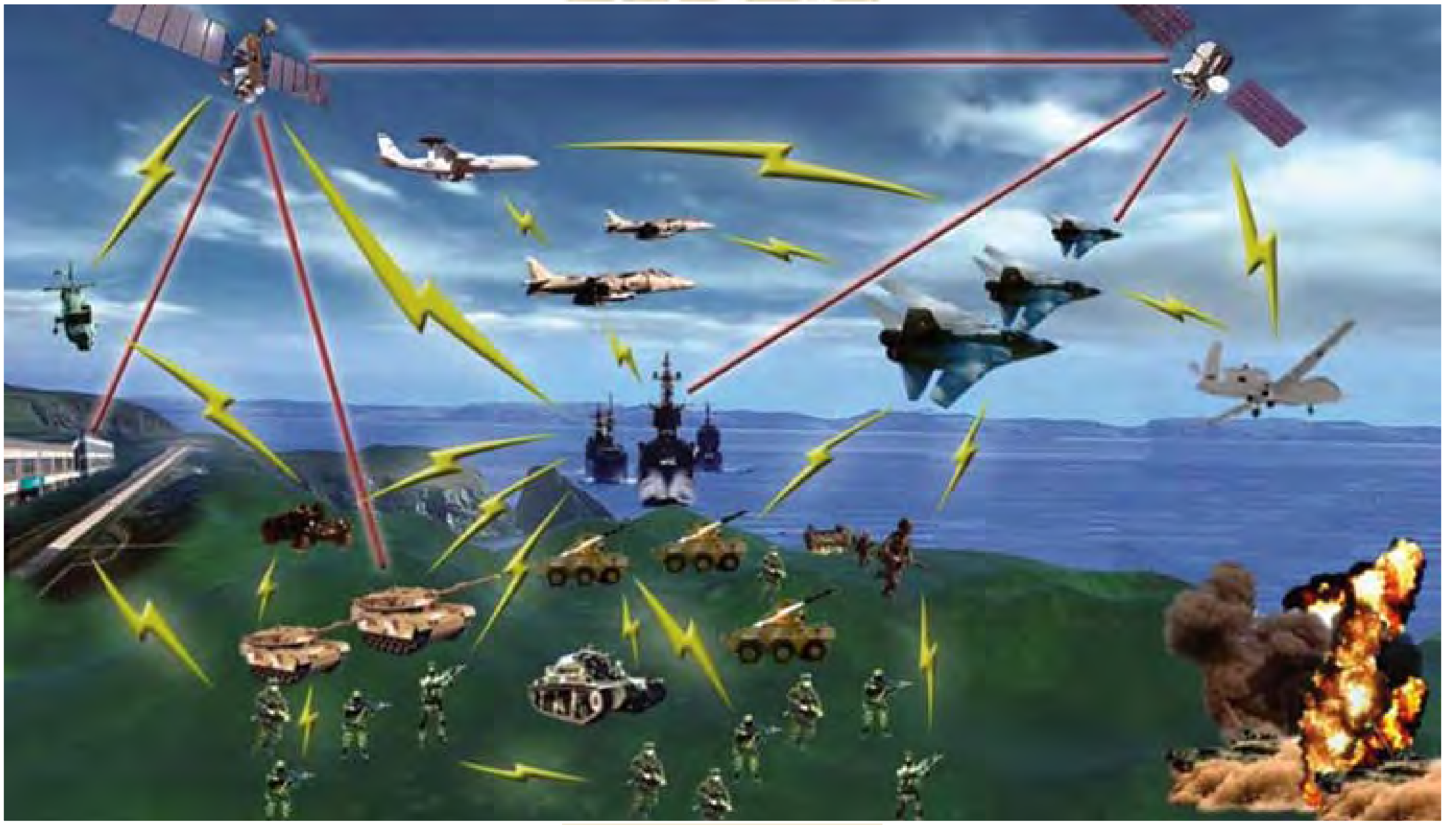
Suffolk USJFCOM
116 Lake View Parkway
Security Office
Suffolk, VA 23435-2697
757.203.7174
FAX 757.203.7512

USJFCOM chairs the Senior Management Group (SMG), the governing body for CWID representing interests of all combatant commands. It is a standing O-6 level group responsible for planning, execution and funding allocation decisions.

The CWID event is an engines for "discovering" solutions for U.S. military, coalition and agency C4ISR challenges. In concert with interoperability trial sponsors and industry representatives, USJFCOM assists with coordination and gathering of information required to support post-execution decisions for promising solutions. During the CWID execution phase, interoperability trials are assessed for technical, security and warfighter attributes. Results of assessments are reviewed and integrated into a senior leadership decision brief. In coordination with the host combatant commander, Joint Staff and SMG leadership, USJFCOM highlights the most promising technology solutions, focusing on near-term benefit to warfighters.

DEFENSE INFORMATION SYSTEMS AGENCY

Lead Agency, Information Technology Delivery for DoD



The Defense Information Systems Agency (DISA) is a combat support agency, responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, the Vice President, the Secretary of Defense, and other DoD components under all conditions of peace and war.

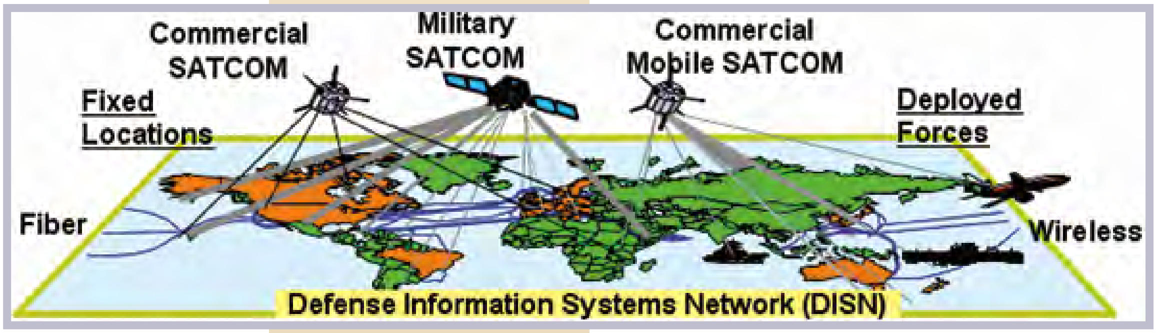
Providing "global net-centric solutions" means much more than superior, jointly interoperable, secure, survivable, and reliable C4 (command and control, communications, and computers) systems. DISA enables global information access and the simultaneous and synergistic employment of air, land, sea, and space warfighting capabilities.

From its Arlington, Va., headquarters and through worldwide field activities, DISA delivers the capability to collect and corre-

CONTACT

Defense Information Systems Agency (DISA)
PO Box 4502
Arlington, VA. 22204- 4502

Lt. Col. Beatriz Westmoreland
Director, CWID
Beatriz.Westmoreland@disa.mil



late data from disparate sources; collaborate with joint, coalition, intelligence, and homeland security communities; and enable them to rapidly turn decisions into strategic, operational, and tactical actions. DISA is unsurpassed in its steadfast commitment to exceeding its customers' requirements by providing solutions and enhanced capabilities that deliver measurable results. Joint cooperation is more than rhetoric at DISA – it is a philosophy and business model that we employ to deliver IT to the sharp edge of the spear.

Three specific areas in which DISA is delivering net-centric services in support of net-centric operations are: 1. Moving toward service-oriented architectures via web services and providing core enterprise services that empower the edge user to pull information from any available source. 2. Optimizing our existing, deployed communications infrastructure, the Defense Information System Network (DISN). 3. Our computing infrastructure will be the hosting facility enabling net-centric operations.

Interoperability and information-sharing are the core of successful joint and coalition operations. All partners — military Services, other government agencies, and coalition partners — must have access to systems that they can "plug into" anytime and anywhere for sharing and for discovery of data and information. These systems must work for a wide variety of missions — e.g., hurricane relief, humanitarian activities, and warfighting.

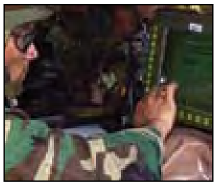
"Our challenges are to establish a standard, common network for coalition missions instead of developing new, unique networks for new missions and to lead the way in the cultural shift from 'need to know' to 'obligation to share.'"

LT. GEN. CHARLES CROOM JR.
DISA DIRECTOR

"Our challenges are to establish a standard, common network for coalition missions instead of developing new, unique networks for new missions and to lead the way in the cultural shift from 'need to know' to 'obligation to share," said Lt Gen Charles E. Croom Jr., DISA's director.

DISA is pleased to serve as the lead agency for CWID. CWID provides an opportunity to work together to improve interoperability and information-sharing. For example, three CWID 2005 programs were successfully deployed by the Department of Defense to support the relief efforts following Hurricane Katrina.

As part of CWID 2006, DISA's goal is to explore using an adaptive and secure coalition research-and-development network architecture, based on communities of interest, that can be easily and quickly scaled and configured to meet diverse multinational requirements associated with operating in an ever-changing coalition environment.



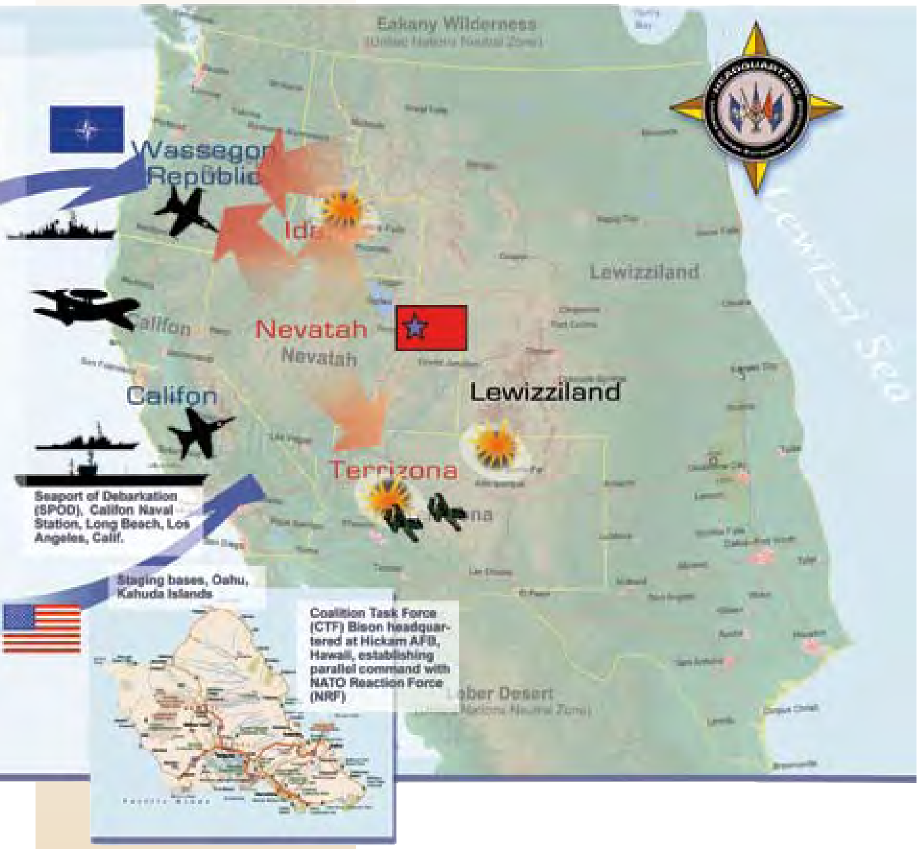
TWO-PART SCENARIO

Scripted Environment for Technology Trials

The scenario describes notional coalition task force operations applicable in the Global War on Terrorism (GWOT) with terrorist backlash and natural disasters for U.S. Northern Command's (USNORTHCOM) Homeland Security and Homeland Defense (HS/HD) component. The simulated operational environment provides context for validation of proposed technology solutions.

DAY 3 IN BRIEF

- ■ Lewizziland Carrier Task Force (CV Sidehorn) reinforces Blu-Blu Surface Action Group (SAG); moves north, crossing 21 degree latitude; maritime patrols increase; Defensive Counter Air (DCA) increased for port of San Diego
- ■ Coalition Task Force (CTF) warns Lewizziland, demands retire south of 21 degree latitude; Coalition Force Maritime Component Commander (CFMCC) prepares to defend Sea Lines of Communication (SLOC)
- ■ Unknown submarine sightings off San Diego and Eureka; presumed Lewizziland
- ■ CFMCC and Coalition Force Land Component Commander (CFLCC) provide Theater Ballistic Missile Defense (TBMD).
- ■ Coalition Force Air Component Commander (CFACC) supports with Close Air Support (CAS), Battlefield Information (BI) and Theater Ballistic Missile (TBM) strikes; Ensures local Air Superiority (AS) over Reno, Nellis operations.
- ■ CFMCC and Marine Forces (MARFOR) prepare for opposed amphibious landing, Corpus Christi.
- ■ 31st Marine Expeditionary Unit (MEU) conducts Ship to Objective Maneuver (STOM), Reno/Tahoe Airport
- ■ CFLCC and Special Operations Forces (SOF); prepare to assault Nellis AFB.



Seaport of Debarkation (SPOD), Califon Naval Station, Long Beach, Los Angeles, Calif.

Staging bases, Oahu, Kahuda Islands

Coalition Task Force (CTF) Bison headquartered at Hickam AFB, Hawaii, establishing parallel command with NATO Reaction Force (NRF)

CTF SCENARIO

U.S. European Command (USEUCOM) is the host Combatant Command for Coalition Warrior Interoperability Demonstration (CWID) 2007.The conflict notionally occurs in Africa on the land mass and littoral of USEUCOM's area of responsibility (actually Western Continental United States). A U.S.-led Coalition Task Force (CTF) and a NATO joint force, NATO Reaction Force (NRF), comprise the friendly forces. The friendly island nation of Kahuda (actually Hawaii) has agreed to provide basing for interim staging and logistical requirements. The CWID 2007 scenario's theme begins with a pre-existent, moderate-sized Terrizona Stabilization Force (TSF) conducting stabilization operations in one nation. Regional unrest then escalates to a regional

MAJOR EVENTS WHEN THE SCENARIO STARTS

- **■ U.S.-led Terrizona Stabilization Force (TSF) in place, Terrizona.**
- ■ CTF Bison is in theater, Oahu, Kahuda Islands; forces marshaled; limited deployment into Area of Operations (southern Arnollia,Terrizona).
- ■ NRF emplaced in area of operations (Wassegon).

DISTRIBUTED TASK FORCE ELEMENTS

COALITION TASK FORCE

U.S. EUROPEAN COMMAND (USEUCOM): Combatant Command; Coalition Task Force Commander; role plays out of Kelley Barracks, Stuttgart, Germany.

COALITION LAND COMPONENT COMMANDER (CFLCC): role plays out of Naval Surface Warfare Center (NSWC), Dahlgren, Va.; U.S. Army and Marine Corps elements of the CFLCC role play out of NSWC, Dahlgren, Va.

COALITION FORCE MARITIME COMPONENT COMMANDER (CFMCC): role plays out of Space and Naval Warfare Systems Command (SPAWAR), San Diego, Calif.

COALITION FORCE AIR COMPONENT COMMANDER (CFACC): role plays out of Electronic Systems Center (ESC), Hanscom Air Force Base, Mass.

NATO RESPONSE FORCE

Command elements of NRF role play out of Camp Jorstadmoen, Lillehammer, Norway

NATIONAL ELEMENTS

Canada, New Zealand, and the United Kingdom role play units from their respective countries; Canada role plays homeland defense with U.S. Northern Command, Colorado Springs, Colo.

multinational insurgency, cross-border invasion and mid-intensity conflict. Destabilization, humanitarian crisis, and hostilities requires the deployment of coalition task forces to reinstate regional stability.

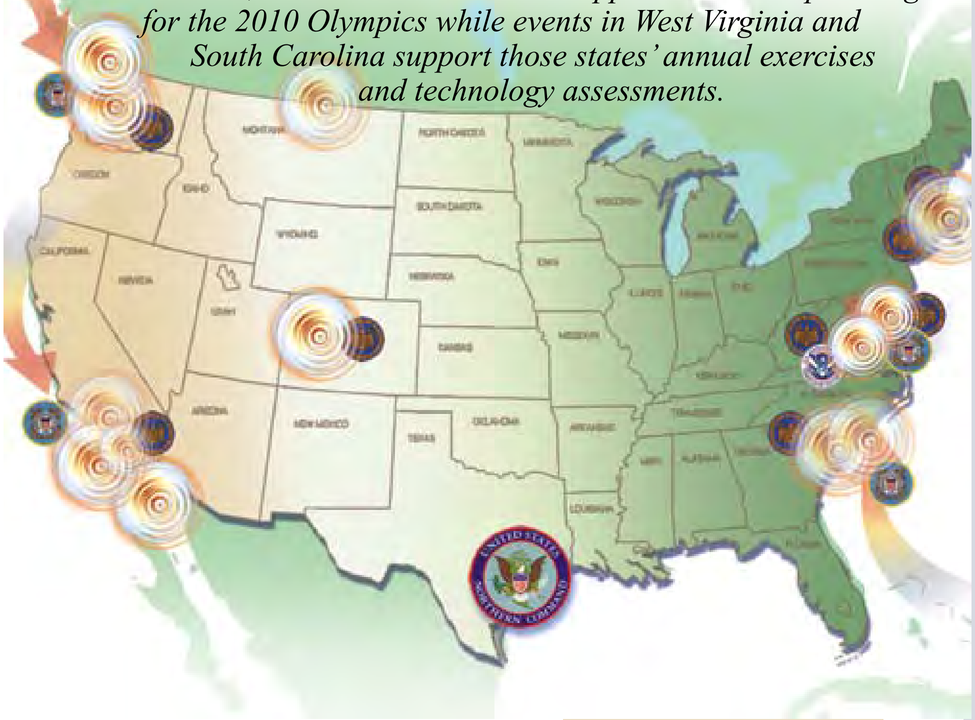
HOMELAND SECURITY/HOMELAND DEFENSE SCENARIO

The Homeland Security/Homeland Defense (HS/HD) scenario supports an on-going interest in technologies that support the Global War on Terrorism (GWOT), and is loosely connected with the CTF Scenario in that it is based on the same worldwide threat. The HS/HD scenario is actually several vignettes within the U.S. Northern Command's Area of Responsibility (AOR). Scenario vignettes provide a broad spectrum of natural and terrorist-related events. The vignettes are focused in areas of the AOR of interest to CWID participants. For instance, events in the northwest support Canadian planning for the 2010 Olympics while events in West Virginia and South Carolina support those states' annual exercises and technology assessments.

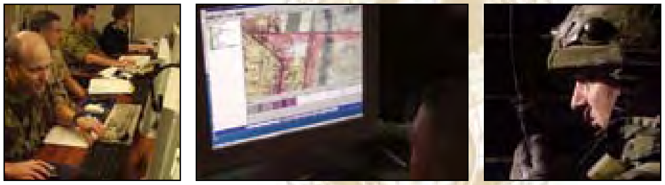
THE HOMELAND DEFENSE MISSION includes participation by USNORTHCOM; U.S. Coast Guard; National Guard Bureau; National Guards of California, Colorado, Delaware, Massachusetts, New York, South Carolina and West Virginia; Department of Justice Seahawk Center; Canada Command; Canadian Government Operations Centre; Canadian Mapping and Charting Establishment; government intelligence liaison officers from both the US and Canada; and the police departments of the cities of San Diego and Colorado Springs.

HS/HD SIGNIFICANT EVENTS OVERVIEW

Vignettes are focused in areas of interest to CWID participants. For instance, events in the northwest support Canadian planning for the 2010 Olympics while events in West Virginia and South Carolina support those states' annual exercises and technology assessments.



- ■ Mass evacuation from Northern Virgina area into West Virginia, surrounding states
- ■ Earthquake, San Diego, Calif.
- ■ Hurricane preparation; landfall, Charleston, S.C.
- ■ Chemical release, NSWC Fallbrook, Calif.,
- ■ Merchant ships missing; one foundoff San Diego with 10kt nuclear device; one found off Charleston, launching cruise missile at city
- ■ Fuel spill, Potomac River
- ■ Attack on refinery; state of Washington
- ■ Anthrax attacks at train stations, Vancouver, BC, and Seattle, Wash.
- ■ Chemical weapon explosion, rail station, Fredericksburg, Va.
- ■ Radiological dispersion device (RDD) threat, San Diego; RDD detonation, Boston, Mass.
- ■ Man Portable Air Defense (MANPAD) threats, San Diego, Seattle, Vancouver
- ■ Truck bombs at power plant, Virginia; PETCO Park, San Diego
- ■ Suspicious ship activity, port of Charleston
- ■ Wildland fires, San Diego; along U.S., Canada border
- ■ Mass evacuation from Mexico as a result of a plague outbreak
- ■ Hostage situation, Colorado Springs, Colo.; high ranking USNORTHCOM official



NETWORK ENGINEERING

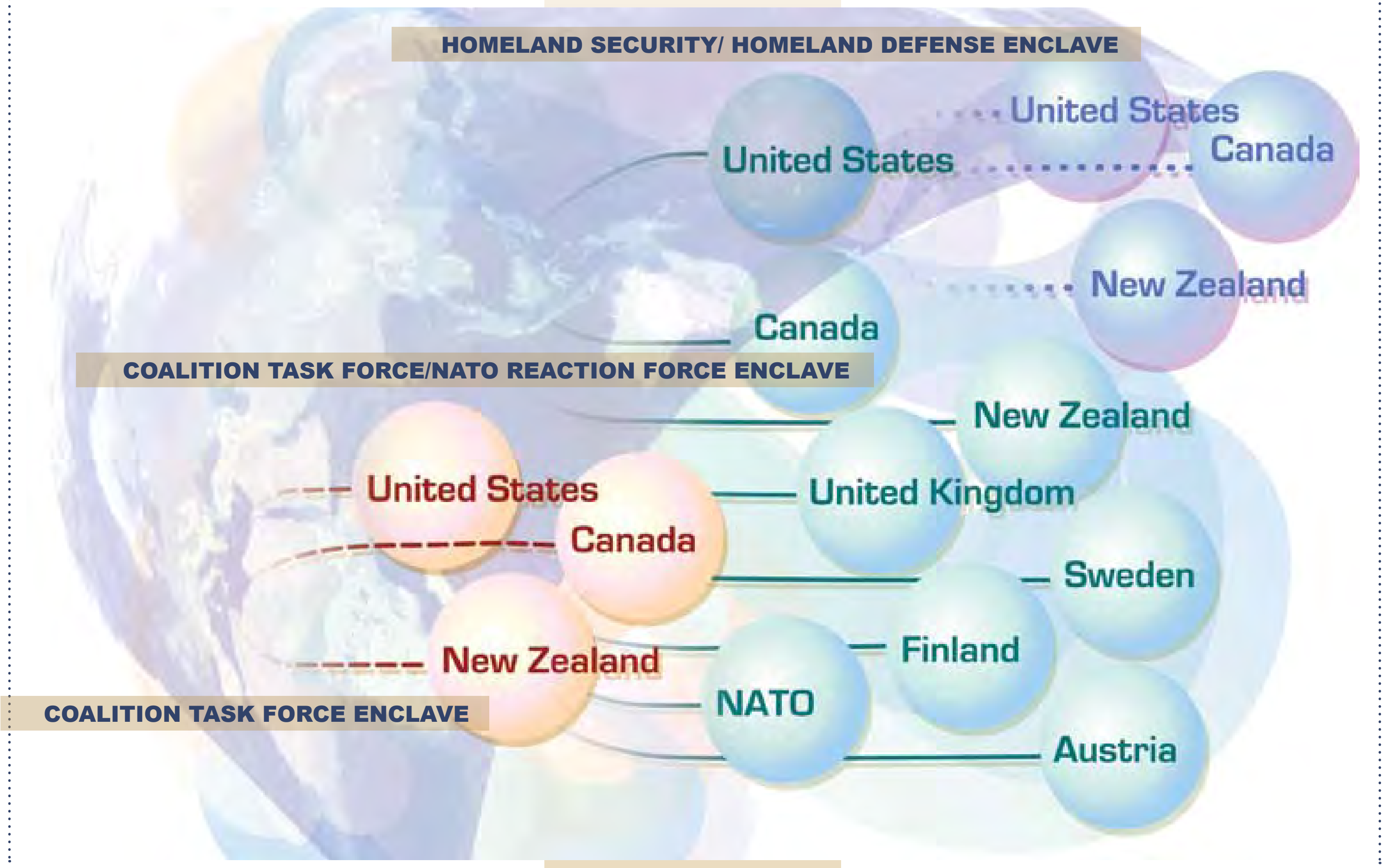
CWID, Connecting the Globe

CWID is the Chairman's annual event to demonstrate the interoperability of cutting-edge technologies. CWID 2007 combines the traditional CWID Warfighter scenarios with Homeland Security and Homeland Defense (HS/HD). In the past, CWID utilized the Combined Federated Battle Laboratories Network (CFBLNet) Blue classified network and the DISN-LES unclassified network.

For 2007, CWID has moved off the DISN-LES and established three enclaves on the CFBL Network. The need for scalability and flexibility drove the development of a new classified coalition information space, called the Coalition Task Force/NATO Reaction Force (CTF/NRF) Enclave. The CTF/NRF Enclave is classified to the level of secret and protected with type-1 encryption devices. This year, CWID is also using the CTF High Enclave to provide a notionally higher classification enclave for Cross Domain Solution (CDS) trials that don't have an approved guard to pass data between unclassified and classified enclaves.

The need for scalability and flexibility drove the development of a new classified coalition information space, called the Coalition Task Force/ NATO Reaction Force Enclave.

In addition to the CTF/NRF and CTF High enclaves, CWID builds and uses an UNCLASSIFIED network to accommodate the interests of U.S. Northern Command (US-NORTHCOM), which sponsors many trials that aim to improve Defense Support to Civil Authorities (DSCA). This enclave, known as the Homeland Security / Homeland Defense (HS/HD) Enclave, represents the network for homeland security while the warfighter enclave represents a secret net-



work for coalition and guest nations.

For the second year, Canada will join the HS/HD Enclave during CWID 2007 and work closely with USNORTHCOM in the testing and evaluation of DSCA technology.

CWID networks use the CFBLNet as the backbone with traffic separated by Type-1 encryption, supporting 30 connection sites in eight nations and NATO. The CTF/NRF Enclave is a temporary security enclave with its own set of services, separate and unique to the CWID environment.

The Multi National information Sharing-Program Management Office (MNIS-PMO) provides an Internet gateway for the HS/HD enclave and, for the first time, maintains a public domain (cwid.org) in order to provide public e-mail access for first responders.

CWID 2007 involves five perennial coalition partners: Canada, New Zealand, United Kingdom, United States, and NATO (the organization). In addition, Sweden, Finland, Germany, France, Italy and Austria are participating in the event this year.

CONTACT

Capt. Ramon Rodriguez
DISA, CWID Network Lead
ramon.rodriguez@disa.mil

U.S. SITES

U.S. EUROPEAN COMMAND

U.S. NORTHERN COMMAND

NAVAL SURFACE WARFARE CENTER, DAHLGREN

SPACE AND NAVAL SYSTEMS COMMAND

MNIS-PMO, ARLINGTON, VA.

HANSCOM AIR FORCE BASE

JOINT INTEROPERABILITY TEST COMMAND

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

DEFENSE THREAT REDUCTION AGENCY

Multinational Information Sharing Joint Program Office

TThe MNIS-JPO, located in Arlington, Va., directly supports and staffs the U.S. portion of the Network Operations Working Group (NOWG) and Security Working Group (SeWG) and hosts the CCCC during CWID each year. The CWID web site, assessment and MSEL servers are also hosted and maintained at the MNIS-JPO.

Support provided by the MNIS-JPO for the NOWG includes engineering and design of the network and services, provisioning of equipment and circuits, and configuration and installation of CFBL nodes. MNIS-JPO supports the SeWG with information assurance, network monitoring, COMSEC, certification and accreditation, and intrusion detection.

This year, Symantec Corporation is providing Intelligence-guided Computer Network Defense (IgCND) system* which, unlike traditional “bastion” network security models, enhances agility and interoperability while improving network security. It provides early warning cyber-intelligence of threats and vulnerabilities before they impact the network, correlated with real-time network sensor information to present the commander and J6 staff with pre-emptive response options.

Sponsors of the MNIS-JPO include the Defense Advance Research Projects Agency (DARPA), the Defense Information Systems Agency (DISA) and the Joint Staff Director for Command, Control, Communications, and computers (JS/J6).

The MNIS-JPO facilitates rapid transfer of advanced information technology from research and experimentation stages to deployment and full-scale implementation within the Global Information Grid (GIG). The MNIS-JPO is a vehicle for implementing long-range information technology strategy and planning among DARPA, DISA and other GIG users, including coalition partners.

The organization also increases project coordination for the rapid insertion of advanced information technology into leading edge pilot services for joint forces and multi-service Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems and software.

The MNIS-JPO supports several Advanced Concept Technology Demonstrations (ACTD) and other information technology-related projects.

CONTACT

Capt. Russel White
DISA MNIS-JPO
russel.white@disa.mil

*For more information on Intelligence-guided Computer Network Defense (IgCND), Symantec Corporation, contact Kent Wilson, 703.373.5410 or 571.423.8603
www.symantec.com

TRIAL ASSESSMENT

Analysts, Agencies Collect Data

The Assessment Working Group's (AWG) charter is to provide the Joint Staff, Command/Services/Agencies (C/S/A), and other interested parties with an objective assessment of warfighter/operator utility, interoperability, and Information Assurance (IA) for Interoperability Trials (ITs).

THE ASSESSMENT PROCESS

The overarching goal of the assessment effort is to identify potential candidates to provide C4I interoperability capabilities or enhancements to Joint, Coalition, and Homeland Security/Homeland Defense (HS/HD) operations.

The AWG consists of three distinct teams, each responsible for assessing a different aspect of the trial as it operates within the CWID environment. The Warfighter/Operator Utility Assessment Team, the Interoperability/Technical Assessment Team, and the Information Assurance Assessment Team. These teams consist of C4ISR Analysts who perform the military utility, interoperability assessments and Information System Security Engineers and Security Testing Specialists, who assess the IA posture of the trials.

The assessment teams independently review each trail to determine the trial's nature, maturity level, and technical factors to define the appropriate level of assessment each trial will receive. In addition, the teams consider the Senior Management Group's (SMG) trial prioritization list when determining how best to apply the AWG's limited resources.

The overarching goal of the assessment effort is to identify potential candidates to provide C4I interoperability capabilities or enhancements to Joint, Coalition, and Homeland Security/Homeland Defense (HS/HD) operations.

During CWID's planning and execution phases, the assessment teams and IT representatives work cooperatively to ensure that the ITs receive objective and meaningful assessments. The assessments include inputs from the operational users and the assessment teams' analysts, testers, and observers. The results of the assessments are captured in various database views, team summaries, and the Final Assessment Report. The Final Assessment Report documents how well the ITs satisfy the applicable CWID objectives in the context of Warfighter/Operator Utility, Interoperability, and Information Assurance. The Final Assessment Report also serves as an input to the overall CWID Final Report.

WARFIGHTER/OPERATOR UTILITY ASSESSMENT PROCESS

The Warfighter/Operator Assessment measures technical performance, the "value added" to warfighters and operators, and the ability of the trial to meet objectives and capabilities in the operational CWID environment. During CWID execution, warfighters, operators and staff interact with trials to gather warfighter/operator feedback and other data. The data required for each IT's assessment is defined prior to execution and is based on:

- How the IT's capabilities map to CWID objectives
- Predefined Master Scenario Events List (MSEL) events and/or definitive test schedules
- Trial capabilities
- Measures of Performance (MOPs) tailored for each trial

INTEROPERABILITY ASSESSMENT PROCESS

The Interoperability/Technical Assessment focuses on an IT's ability to exchange usable data with CWID network services or other trials. During CWID planning, the Interoperability Assessment Team works with each trial's representatives to define Information Exchange Requirements (IER) based upon system interfaces, anticipated data exchanges, and their mapping to CWID objectives. IERs define what information is exchanged, who exchanges the information, why the information is necessary, and how the exchanges take place.

During execution, the Interoperability Assessment Team observes whether or not data is transferred to, and processed correctly by, the receiving system. Results are then documented in the JITC's WISE Interoperability Collection Assessment Tool (WICAT) database. Applicable portions of this database are delivered to the trials during the reporting phase. All information collected by the Interoperability Assessment Team can be used to support the formal U. S. Interoperability Certification Process, potentially expediting product fielding.

The Assessment Working Group consists of three distinct teams, each responsible for assessing a different aspect of the trial:

■

Warfighter/Operator Utility

■

Interoperability/ Technical

■

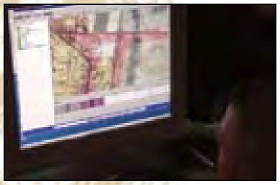
Information Assurance

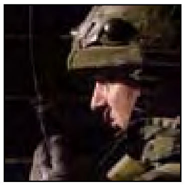
INFORMATION ASSURANCE ASSESSMENT PROCESS

The IA Team performs varying levels of analysis during CWID's planning, execution, and reporting phases. During the planning phase, the team performs an analysis of the trials' capabilities to determine an appropriate level of the assessment for each trial. Trials will be eligible to receive one of three types of IA Assessments: Basic, Conceptual, or Targeted. Trials that connect equipment to select CWID networks during execution will receive a Basic Assessment; this is a simple, non-intrusive discovery scan using tools such as Retina, Nessus, Network Mapper (NMAP), and Kismet. U. S.-sponsored trials with IA functionality may receive a Conceptual or Targeted Assessment. The Conceptual Assessment records and analyzes vendor claims of information security. The Targeted Assessment provides not only the analysis of the conceptual assessment, but also uses testing and discovery tools to substantiate the vendor's claims.

Data collected during execution will shape the IA Team's input to the final report. IT vendors should be able use the results of the IA Assessment to garner a sense of their product's security posture.

NOTES





TRIAL MATRIX

Cross Reference Trials to Sites

CWID trials for 2007 are listed in trial number order below, cross referenced to sites where they can be observed during the demonstration 12 to 21 June. For short descriptions of each trial, go to the TRIALS tab. Refer to the trials contents page at the beginning of the section to locate particular summaries.

OBJECTIVES KEY

1. CROSS-DOMAIN DATA SHARING ■
2. INTEGRATED INTELLIGENCE ■
3. INTEGRATED OPERATIONS ■
4. INTEGRATED LOGISTICS ■
5. INTEGRATED PLANNING ■
6. INTEGRATED COMMUNICATIONS ■

TRIAL NO.	SYSTEM TITLE (ACRONYM OR SHORT NAME)	USEUCOM	USNORTHCOM	DAHLGREN	SPAWAR	HANSCOM	CANADA	NEW ZEALAND	UNITED KINGDOM	NATO	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	OBJECTIVE/S ADDRESSED	PAGE NO.
IT01.01	Compartmented High Assurance Information Network (CHAIN)	■	■	■	■	■					USNORTHCOM	Raytheon	1,3,4,5	3
IT01.05	Trusted Gateway System (TGS) Guard				■	■		■			US Air Force	US Air Force	1	3
IT01.17	Cross Domain Collaborative Information Environment/Collaboration Gateway (CD-CIE/CG)	■	■	■				■			US Air Force, USJFCOM, FBI	Trident Systems, Inc., leads more than 12 other companies	1,2,3,5	4
IT01.28	NET/X eToken Security System, Deployable Communicartions System (NET/X)		■	■	■						USJFCOM	FED-COMM USA, Inc.	2	4
IT01.43	Mobile Forces Solution - Subnet Relay (MOFS-SNR)				■					■	Germany	T-Systems Enterprise Services GmbH	1	5
IT01.54	Collaborate-Access-Browser (CAB)	■	■	■	■	■		■			NSA	Essex Corporation	1	5
IT01.55	Assured File Transfer (AFT)	■		■	■	■		■			NSA	CTC, Essex Corporation,Tresys Technology	1	6
IT01.56	Dual Diode (One-Way) Data Transfer System (Dual Diode)				■		■	■			Canada	Owl Computing Technologies, Inc.	1	6
IT01.61	INTEGRITY Secure Workstation (INTSecWS)						■				Canada	Green Hills Software, Inc.	1	7
IT01.63	Coalition Assured Sharing Environment (CASE)		■	■							DISA	General Dynamics	2	7
IT01.86	Federated Identity Mangement System (FIDMS)		■	■		■					USJFCOM	BearingPoint, Hewlett Packard	1	8
IT01.87	Federated Security (FS)			■							USJFCOM	SAIC, IBM, Sun	2	9
IT02.06	Italian Navy Maritime Command and Control Information System (MCCIS-Italy rel. 5.2)				■					■	Italy	MARITEL-Roma	2	9
IT02.16	Deployable Geospatial Database (DGDB)		■				■				Canada	Canada	2	10
IT02.21	Commercial Joint Mapping Tool Kit (CJMTK)		■	■	■				■		NGA	Northrop Grumman Corporation	2	10
IT02.37	Rapid Force Warning (RFW)					■				■	US Army	US Army	2	11
IT02.57	Automatic Ingest, Mosaic and Mapping System (AIMM)		■	■	■		■				Canada	PCI Geomatics.	2	11
IT02.88	AdLib			■					■		USNORTHCOM	EchoStorm, Inc.	2	12
IT03.09	Global Personnel Recovery System (GPRS)	■	■	■							USJFCOM	Innovative Solutions International	2,3,4,5	12
IT03.14	Coalition Secure Management and Operations System (COSMOS)	■		■			■		■	■	OSD, USEUCOM, DISA	DISA, NSA, CDM	3,6	13
IT03.22	Scalable Mesh Networks				■						US Navy	OrderOne Networks	3,2	13

Continued next page

OBJECTIVES KEY

1. CROSS-DOMAIN DATA SHARING ■
2. INTEGRATED INTELLIGENCE ■
3. INTEGRATED OPERATIONS ■
4. INTEGRATED LOGISTICS ■
5. INTEGRATED PLANNING ■
6. INTEGRATED COMMUNICATIONS ■

TRIAL NO.	SYSTEM TITLE (ACRONYM OR SHORT NAME)	USEUCOM	USNORTHCOM	DAHLGREN	SPAWAR	HANSCOM	CANADA	NEW ZEALAND	UNITED KINGDOM	NATO	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	OBJECTIVE/S ADDRESSED	PAGE NO.
IT03.27	Integrated Information Management System (IIMS)			■							US Army, US Air Force	US Army, US Air Force	**3**	**14**
IT03.30	Spatio-Temporal Analysis for Rapid Tasking (START)					■					US Air Force	The MITRE Corporation	**3**	**14**
IT03.31	Coalition Infrared Data Processing (CIDP)	■		■					■		US Air Force	Space and Missile Center, Missile Defense Agency	**3**,5	**15**
IT03.38	Collaborative Decision Aid (CDA)		■	■			■				USNORTHCOM	ARINC Engineering Services, LLC	**3**,5	**15**
IT03.39	Command, Control, Communications, Computers and Intelligence Defense (C4I Defense)	■		■		■	■				Italy	SELEX-SI SpA	**3**	**16**
IT03.48	Air Support Operations Center with Close Air Support System (ASOC Gateway with CASS)			■							US Air Force	US Air Force, US Navy	**3**	**16**
IT03.58	US Coast Guard Information Sharing and Communications (USCG IS&C)		■	■							US Coast Guard	US Coast Guard	**3**	**17**
IT03.70	Coalition open Joint Operations Picture (CoJOP)	■		■	■	■	■	■	■		UK	Fujitsu Services	**3**,5	**17**
IT03.71	MobiKEY Identity Based Access Drive (MobiKEY IBAD) and Defense Identity Management Network (DEFIMNET)	■	■	■	■	■	■	■			Canada	Route1, Inc.	**3**,5	**18**
IT03.75	Mobile Tactical Edge Network (MTEN)		■	■							USNORTHCOM	Professional Software Engineering, Inc., pTerex, LLC	**3**	**18**
IT03.80	Riverbed Information Optimization System (RIOS)	■	■	■		■		■			US Air Force, DISA	C2I Solutions, Riverbed	**3**,4	**19**
IT04.79	Event-based Common Operational Picture (ECOP)		■	■	■	■					NGB	Booz Allen Hamilton	**3**,4,5	**19**
IT05.08	Joint Strike Fighter (JSF) Offboard Mission Support Environment (OMSE)			■		■			■		JSF Program Office	Lockheed Martin, Systematic Software Engineering, Naval Mission Planning	**5**,1	**20**
IT05.12	ID-MAP: Situational Awareness, Visualization and Collaboration (ID-MAP)		■	■	■						USNORTHCOM, US Coast Guard	General Dynamics	**5**,2,3	**20**
IT05.59	Mission Planning System (MPS)					■	■	■			US Air Force	Collaboration Technologies, Inc.	**3**,5	**21**
IT05.78	Next Generation - Joint Information Exchange Environment (NG-JIEE)		■	■	■	■					NGB	Koniag Services, Inc.	**5**	**21**
IT06.04	Tactical Emergency Asset Management (T.E.A.M.)		■		■						USNORTHCOM	Quantum Research International	**6**	**22**
IT06.13	Global Information Grid Quality of Service Edge Solution for Interoperability (GIG QoS ESI)			■	■			■			US Army	DSCI	**6**	**22**
IT06.15	Geolap		■				■		■		Canada	Canada	**6**	**23**
IT06.36	Joint Network Defense and Management System (JNDMS)						■				Canada	MacDonald Dettwiler and Associates (MDA)	**6**	**23**
IT06.42	HotZone 4010/4020 (HZ4010)				■						US Navy	Trimax Wireless, Inc.	**3**,6	**24**
IT06.53	Weapons of Mass Destruction Collaborative Advisory Response System (WMD CARS)	■	■		■	■					USNORTHCOM	Defense Threat Reduction Agency (DTRA)	**3**,**5**	**24**
IT06.66	Internet Protocol Interoperability and Collaboration System (IPICS)		■	■			■				Canada	Cisco Systems, Inc.	**6**	**25**
IT06.74	Security Information Management for Enclave Networks (SIMEN)		■	■		■		■			US Air Force	The MITRE Corporation	**1**,6	**25**
IT06.89	Enhanced Video Text and Audio Processing (eVITAP)		■	■	■		■	■			US Joint Staff	Virage Inc.	**6**	**26**
IT06.90	Optimized Data Environment for NetCentric Operations (ODEN)		■	■	■						DISA	TIMMES, Inc.	**6**	**26**
History of Coalition Warrior Interoperability Demonstration														**27**
Abbreviations and Acronyms, inside back cover														